UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,211	03/16/2004	Russell C. Blaisdell	RSW920040023US1	2031

25259 7590 10/26/2007

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
WILLIAMS, CLAYTON R	
ART UNIT	**PAPER NUMBER**
4152	

NOTIFICATION DATE	DELIVERY MODE
10/26/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

RSWIPLAW@us.ibm.com

Office Action Summary	Application No.	Applicant(s)	
	10/801,211	BLAISDELL ET AL.	
	Examiner	Art Unit	
	Clayton Williams	4152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *03/16/04* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/16/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-6 are pending in this application.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claim 1, 3, 4, 5 and 6 are rejected under 35 U.S.C. 102(e) as being anticipated by Gales (U.S. Publication No. 2003/0084323 A1).

Regarding claim 1, Gales clearly shows and discloses a method suitable for filtering events in an information technology resource monitor, comprising: determining a present count of occurrences of an event for a present monitoring period (Fig. 3; [0021], lines 1-5);

comparing the present count with numbers of occurrences of the event in a plurality of earlier monitoring periods (Periodically, the profile application acquires network activity log, which is generated by monitoring application, and uses this data to generate activity profile. The recognition engine then compares this activity profile against future network activity.)([0022], lines 1-6 and 11-17; [0023], lines 2-5);

invoking a first action if the present count exceeds a predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods ([0023], lines 9-13; Fig. 3, items 214 and 216); and

invoking a second action if the present count does not exceed the predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods ([0025], lines 1-5; Fig. 3, item 214, loopback).

Regarding claim 3, Gales clearly shows and discloses the method of claim 1, wherein the second action includes logging the present count without taking further corrective action (The monitor application records the events it is monitoring to a network activity log, which is later incorporated into a network profile. Both the log and profile are stored as databases, and further action beyond logging is only taken in the event the recorded events exceed a threshold which invokes the first action.)([0014], lines 11-15; [0016], lines 1-6).

Regarding claim 4, Gales clearly shows and discloses the method of claim 1, wherein the plurality of earlier monitoring periods all begin at the same times on consecutive days previous to the present monitoring period. (Gales teaches the activity profile being updated in accordance with predefined time periods.)([0022], lines 11-15).

Regarding claim 5, Gales clearly shows and discloses a program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps suitable for filtering events in an information technology resource monitor, said method step comprising:

determining a present count of occurrences of an event for a present monitoring period ([0014], lines 1-3 and 6-13);

comparing the present count with numbers of occurrences of the event in a plurality of earlier monitoring periods ([0014], lines 15-18);

invoking a first action if the present count exceeds a predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods ([0014], lines 18-21); and

invoking a second action if the present count does not exceed the predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods (Gales teaches different actions being performed based on whether events recorded in activity log exceed threshold established in activity profile.)([0014], lines 15-18; [0018], lines 8-12).

Regarding claim 6, Gales clearly shows and discloses a filter suitable for filtering events in an information technology resource monitor, said filter comprising:

an event counter for determining a present count of occurrences of an event for a present monitoring period (Fig. 3; [0021], lines 1-5);

a history table for storing numbers of occurrences of the event in earlier monitoring periods (The activity log, which records events logged during time periods, is stored in a database.) (Fig. 2; [0016], lines 1-4); and

logic for comparing the present count with numbers of occurrences of the event in a plurality of earlier monitoring periods selected from the history table, invoking a first action if the present count exceeds a predetermined proportion of the numbers of

occurrences of the event in the plurality of earlier monitoring periods, and invoking a second action if the present count does not exceed the predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods (Fig. 2; [0014], lines 16-21; [0016], lines 1-6).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gales in view of Porras et al. (US Publication No. 2004/0010718 A1), hereinafter referred to as Porras.

Regarding claim 2, Gales clearly discloses a method for filtering events in an information technology resource. However, Gales does not disclose a method wherein the predetermined proportion is a majority.

In the same filed of endeavor, Porras does clearly show and disclose a method of employing a wide range of statistical measures to compare the number of occurrences of events in a current monitoring period with the number of occurrences of events in past monitoring periods, reading on the claimed "wherein the predetermined

proportion is a majority," ([0035], lines 1-3; [0040]). In light of computer networks becoming more sophisticated and interoperable and subject to both increasing levels of reliance by users and malicious and coordinated attacks, the method of Porras to perform comparisons using a range of statistical measures was within the ordinary ability of one motivated to improve upon methods of detecting suspicious network activity and, more generally, networking monitoring (Porras: [0005]; [0006]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the statistical comparison methods taught by Porras with the method of Gales in order to filter events to obtain the invention specified in claim 2.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Rowland, (U.S. Patent No. 6,405,318)

Weber et al., (U.S. Publication No. 2006/0173992)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Clayton Williams whose telephone number is 571-270-3801. The examiner can normally be reached on M-F (7-30 a.m. - 5 p.m.).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nabil El-Hady can be reached on 571-272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CW 10/22/07

WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100